Tle

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,802	12/12/2003	David M. Chess	YOR920030570US1	3904

7590 03/23/2007

Moser, Patterson & Sheridan
Suite 100
595 Shrewsbury Avenue
Shrewsbury, NJ 07702

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	PAPER NUMBER
2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/734,802	**Applicant(s)** CHESS ET AL.
	Examiner James Turchen	**Art Unit** 2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 12 December 2003.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-30 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-30 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 12 December 2003 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) □ Notice of Informal Patent Application
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 03/12/2004.	6) □ Other: _____.

DETAILED ACTION

1. Claims 1-30 are pending.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3, 5-8, 13-17, 23-25, and 27-30 are rejected under 35 U.S.C. 102(e) as being anticipated by Baffes et al. (US 2004/0111636).

Regarding claim 1:

Baffes et al. discloses a method for automated adaptive reprovisioning of servers under security assault, the method comprising: detecting a security assault or a possible security assault on a first server (paragraph 38, step 302); and reprovisioning by automatically creating a new server instance with a desired new server configuration to perform at least one of the tasks performed by said first server (paragraph 0038, step 306, the server is reprovisioned as a honeypot).

Regarding claim 2:

Baffes et al. discloses the method of claim 1, wherein said detecting comprises determining if said first server is a candidate for reprovisioning, because of properties or behavior that suggest its security has been compromised or is likely to be compromised, or its functioning otherwise unacceptably impaired, by a security assault (figure 3, shows that reprovisioning will only occur when and intrusion is detected).

Regarding claim 3:

Baffes et al. discloses the method of claim 1, wherein said reprovisioning comprises automatically bringing up said new server instance, or otherwise making available said new server instance to customers or other users of said first server (paragraph 0039 and 0040, the honeypot could be reprovisioned to various levels of "decoy-ness", allowing other users (servers) in the farm to have access to it. Additionally, there server may revert back to it's original state (examiner considers this to be the second instance of server reprovisioning)).

Regarding claim 5:

Baffes et al. discloses the method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server in at least one parameter (figure 3, step 306, the server is brought up as a honeypot upon being compromised).

Regarding claim 6:

Baffes et al. discloses the method of claim 1, wherein a difference between said new server instance and said first server is responsive to whether or not other security incidents have been detected in a network to which said servers are coupled (paragraph 0033, intrusion detector 208 detects an intrusion within the networked server farm 100; figure 3, steps 302-306).

Regarding claim 7:

Baffes et al. discloses the method of claim 1, wherein a difference between said new server instance and said first server is responsive to a nature of any other security incidents that have been detected in said network to which said servers are coupled (paragraph 0033, intrusion detector 208 detects an intrusion within the networked server farm 100; figure 3, steps 302-306).

Regarding claim 8:

Baffes et al. discloses the method of claim 1, wherein a difference between said new server instance and said first server is responsive to a probable compromise or a functional impairment observed in said detection (paragraph 0033, intrusion detector 208 detects an intrusion within the networked server farm 100; figure 3, steps 302-306).

Regarding claim 13:

Baffes et al. discloses the method of claim 1, wherein a difference between said new server instance and said first server includes a degree of function offered to users by said servers (paragraph 0039 and 0040, the honeypot could be reprovisioned to various levels of "decoy-ness").

Regarding claim 14:

Baffes et al. discloses the method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server only if more than a fixed number of instances of probable server compromise have been observed (figure 3, steps 302-306 and paragraph 0038 disclose the reprovisioning occurring after the first intrusion, examiner interprets the fixed number to be zero).

Regarding claim 15:

Baffes et al. discloses the method of claim 1, wherein a difference between said new server instance and said first server is responsive to a number of probable server compromises that have been observed (figure 3, steps 302-306 and paragraph 0038 disclose the reprovisioning occurring after the first intrusion, examiner interprets the fixed number to be zero).

Regarding claim 16:

Baffes et al. discloses the method of claim 1, wherein said server comprises a computer providing services through a network (paragraph 0024, servers 102, servers are inherently computers providing services through a network).

Regarding claim 17:

Baffes et al. discloses the method of claim 1, wherein said server comprises a program running on a network-coupled computer, providing services through a network (paragraph 0024, servers 102, servers are inherently computers running programs that provide services through a network).

Regarding claims 23-25 and 27-29:

Claims 23-25 and 27-29 disclose the method claims 1-3 and 5-7 on a computer readable medium and are therefor rejected by the same reasoning as claims 1-3 and 5-7.

Regarding claim 30:

Baffes et al. discloses a system for automated adaptive reprovisioning of servers under security assault, the system comprising: a first server; a security monitor (figure 2a, item 210), coupled to said first server (figure 2a, the lines connecting the machines to intrusion manager), for detecting if said first server is a candidate for automatic reprovisioning with a new server instance (paragraph 0034, intrusion 206 causes intrusion manager 210 to notify response coordinator 212 which instructs reprovision manager 216 to begin reprovisioning); and a provisioner (figure 2a, item 216), coupled to said first server (figure 2a, the lines connecting the machines to provisioning manager), for automatically reprovisioning said server with said new server instance if said server is such a candidate (paragraph 0034, intrusion 206 causes intrusion manager 210 to notify response coordinator 212 which instructs reprovision manager 216 to begin reprovisioning).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims rejected under 35 U.S.C. 103(a) as being unpatentable over Baffes et al. as applied to claim 1 above, and further in view of Agha et al. (US 6,044,461).

Regarding claim 4:

Baffes et al. discloses the method of claim 1, but does not teach bringing down first server prior to said reprovisioning. Agha et al. teaches restarting the system into a maintenance mode before processing code updates (figure 3). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method for reprovisioning a server of Baffes et al. with the code update method of Agha et al. in order to allow the code updates to be installed (column 2, lines 21-28).

Regarding claims 9-12:

Baffes et al. discloses the method of claim 1, but not teach the difference between said new server instance and said first server includes a version of operating system software used by said servers. Agha et al. teaches updating program code wherein program code "generally includes the operating system of the computer system, as well as any lower-level program code utilized by the computer system, including microcode, basic input/output system (BIOS) program code, kernel program code, startup program code, etc" (column 1 lines 18-22). Changing strength of encryption would have been obvious to one of ordinary skill in the art in order to further protect the server's incoming and outgoing communications. It would have been obvious to one of ordinary skill in the art to combine the reprovisioning method of Baffes et al. with the method for updating program code of Agha et al. in order to update the system (column 1 lines 6-9).

Regarding claim 26:

Claim 26 discloses method claim 4 on a computer readable medium and is therefor rejected by the same reasoning as claim 4.

4. Claims 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baffes et al. as applied to claim 1 above, and further in view of Burnett et al. (US 2003/0018889).

Baffes et al. discloses the method of claim 1, but does not disclose selecting said new server instance from a plurality of new server configurations. Burnett et al. discloses selecting a configuration from a configuration database, 135, in paragraph 0049. Using a table and randomly selecting the configuration are obvious variations of selecting the new server configuration. Examiner interprets claim 22 as selecting a table after a number of times a server has been subject to probable compromise (in the reference, the number of times is equal to one). It would have been obvious to one of ordinary skill in the art to combine the method of Baffes et al. for reprovisioning a server with the configuration database of Burnett et al. in order to store all of the configurations.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art discloses detecting intrusions, responding to intrusions, software distribution and updates, and configurations.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100